

# National Infrastructure Advisory Council (NIAC)

## The Insider Threat to Critical Infrastructures

**Thomas Noonan**  
General Manager  
IBM Internet Security Systems

**Edmund Archuleta**  
General Manager  
El Paso Water Utilities

## Overview

- Objective
- Report findings highlights:
  - Defining the Insider Threat
  - Scope: Psychology and the Disgruntled Insider; Variation on Maturity and Awareness
  - Dynamics: Technology and Globalization
  - Obstacles to addressing the Insider Threat
  - Developing recommendations
- Next Steps
- Questions

## Objective

---

- First Phase focused on defining the insider threat to critical infrastructures, including dynamics involved, obstacles to mitigation, and the effect of globalization
- The second phase of the study will focus on legal, procedural, and policy barriers for private sector infrastructure operator employee screening efforts
- Completion of the study may produce potential recommendations for improving operators' ability to address the insider threat to critical infrastructures, and seek to provide guidance on a clear legal environment for operators in dealing with potentially hostile insiders

3

## Defining the Insider Threat

---

Definition: *the Insider Threat to critical infrastructure is an individual with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm*

- Critical Infrastructure-level threats affect
  - Critical infrastructure services delivery
  - National economic back-bone
  - Public health and safety
- Potential risk for each employee is based on:
  - Access to critical systems
  - Knowledge of critical systems and vulnerabilities

4

## Insider Threat: Scope

---

- ❑ Risk Management approach to protection: based on informed understanding of threat, vulnerability, and consequence
  - Identify and prioritize risks based on identification of critical assets
- ❑ Understanding threats
  - Actors and motivations
  - Importance of psychology and the “disgruntled” insider
  - Emerging Economic Espionage threat
- ❑ Variation on maturity and awareness of the insider threat

5

## Scope: Importance of Psychology and the “Disgruntled” Insider

---

- ❑ The psychology of the “disgruntled” insider plays a role in understanding almost all insider threat cases
  - CERT/CC-US Secret Service study found commonalities between U.S. espionage cases and known cases of “disgruntled” insiders committing acts of IT sabotage
  - The Working Group is investigating links between disgruntled insider psychology and workplace violence cases
  - Needs more research
- ❑ The vast majority of disgruntled employees are not potential insider threats
- ❑ Common characteristics and common path to betrayal
  - Not a profile – a critical pathway

6

## Scope: Variation on Maturity and Awareness of Insider Threats

---

- ❑ Awareness of the insider threat varies greatly among the critical infrastructure sectors
- ❑ Need baseline, common understanding of the risks for owner-operators
  - Misperception of risk can result in complacency and denial
  - Aware, but do not fully understand the risks and potential consequences
- ❑ To get CI owner-operators to actively manage insider risks:
  - Need common, clear understanding of the threat
  - Achievable, cost effective mitigation goals
- ❑ Need improved information on what is happening with insider incidents
  - Improved information sharing for better data and research – business intelligence level information
  - Effective communication of government threat information to owner-operators

7

## Dynamics of the Insider Threat

---

- ❑ Technology and globalization risks are intertwined
- ❑ Industry is immature at detecting insiders
- ❑ Technology risks for companies are growing at a rapidly escalating rate – faster than the solutions
- ❑ Existing insider threat tools are expensive to deploy
- ❑ Significant, escalating technology threats:
  - Proliferation of small, mobile computing devices and constant network access are eroding traditional workplace boundaries
  - Threat tools are increasingly commonly accessible and easy to use, reaching greater group of potential insiders

8

## Globalization

- ❑ Globalization affects different sectors in different ways and to different degrees
- ❑ Emerging globalization risks include:
  - Expanding the group of trusted insiders within a company to new populations – less verifiable, different cultural norms
  - Emerging global supply chain vulnerabilities
- ❑ Multinational corporations face legal obstacles
  - Legal deterrence for insider betrayal, Intellectual Property and patent protections, and enforcement of laws all can vary significantly

9

## Obstacles to Addressing the Insider Threat

- ❑ Information Sharing on insider threats
  - No reliable threat intelligence
  - No trusted entity for collection and protection
  - Little incentive to share information on insider incidents
- ❑ Education and Awareness
  - Need baseline understanding of insider threats
  - Need effective mitigation programs
  - Key to needed cultural change
- ❑ Background Investigations
  - Not universally accepted, no standard or common method
  - Periodic reinvestigation or monitoring for critical positions
- ❑ Technology
  - Threat tools growing faster than the solutions
  - Need more deployable, adaptable solutions
- ❑ Cultural and Organizational obstacles
  - Collaboration needed between IT, HR, Security, and asset owners to address insider threats
  - Culture and institutional momentum can hinder mitigation (unquestioned trust of long-time employees)

10

## Developing Recommendations

---

Plan to develop specific, actionable recommendations to address identified obstacles:

- ❑ Information Sharing
  - Need government intelligence agencies to share relevant strategic level information on insider threats
  - Sectors need to establish a trusted process and mechanism to share incident information
  - Need an insider threat clearinghouse/resource for owner/operators seeking to assess and mitigate their insider risks
- ❑ Education and Awareness Framework
  - Executive and workforce education and awareness of insider threats
  - Senior Management implementation for affecting cultural change
- ❑ Background Investigations
  - Exploring during Phase II study
  - Examining the challenges facing infrastructure operators in developing risk-focused background investigation programs
- ❑ Technology
  - Investigating needed technology solutions
  - Has potential role in mitigating insider risks
- ❑ Cultural and Organizational Obstacles
  - Under Investigation

11

## Next Steps

---

- ❑ Begin *Phase II* research
- ❑ Working Group finalize *Phase I* Report
- ❑ Research and develop specific, actionable recommendations for identified obstacles
- ❑ Write *Phase II* Report
- ❑ Publish Final Report at January 2008 meeting

12



---

# Questions?